ABSTRACT:

The invention relates to an encryption method as well as to an encryption device wherein at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words and wherein the relevant result or relevant intermediate results y_i are digitally stored or buffered as data bit words. At option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to $\overline{x}_i$, $\overline{k}_i$ and/or $\overline{y}_i$ or not, depending on a control signal r_i which is based on random numbers.

Fig. 2